HARRIS
Electronic Systems

HARRIS CORPORATION
Information Systems Division

JA #1486

Network Visualization Tool (NVT)

Task #3 Report: Comparison of COTS Vulnerability Assessment/Reasoning Engines for Automated Reasoning

Contract #F30602-96-C-0289

Mr. Dwayne P. Allain
AFRL/IFGB
425 Brooks Road
Rome, NY 13441-4503

Table of Contents

ABSTRACT: 1

1.0 Introduction 1

2.0 Survey of Vulnerability Assessment and Reasoning Tools 2

3.0 Tool Evaluation Criteria 2

4.0 Selection Process 6

5.0 Recommendation 9

Appendix A - Vulnerability Assessment Technologies Summary 1

ABSTRACT:

This paper documents the findings of Task Three - Automated Reasoning of the Network Visualization Tool (NVT) program. Task Three, Automated Reasoning, identified and evaluated available commercial-off-the-shelf (COTS), government-off-the-shelf (GOTS), and evolving research vulnerability assessment and reasoning tools for applicability as integrated automated reasoning engines for the NVT program prototype. The evaluation criteria included assessment capability, output type, type of vulnerability assessed, data acquisition method, platform operability, and applicability for the NVT program prototype. Three vulnerability assessment reasoning tools, reflecting three different types of reasoning engines, are recommended for inclusion in the NVT prototype.

1.0 Introduction

The Network Visualization Tool program is based on the concept of a knowledge solicitation framework that incorporates a graphical description of a network topology. This topology is used for capture of network attributes, and is subsequently analyzed for security vulnerabilities. The knowledge solicitation portion of NVT uses modern network discovery capabilities and a graphical user interface to increase the accuracy of the network model, provides a common network description for multiple risk analysis reasoning engines, and enhances the productivity of the system security analyst. The NVT program should provide a single topological model supporting the information needs of multiple reasoning tools. In addition to collecting information for input into the reasoning tools, NVT can be used to highlight the vulnerabilities identified by the various reasoning tools. Therefore it is desirable that the vulnerability assessment and reasoning tools have data acquisition and data output formats that are easily adapted to knowledge solicitation portion of NVT.

NVT Task Three-- Automated Reasoning surveyed the current vulnerability assessment and reasoning tools to determine their capabilities and availability. These tools were categorized by the types of vulnerabilities assessed and the functional tool characteristics. Each tool was further evaluated on its data acquisition and output formats to determine how the information can be applied in the NVT prototype implementation. The trade survey methodology is outlined in Section 2.0 of this paper. The characterizations developed during the evaluation are described in Section 3.0 of this paper. Section 4.0 describes the selection process and the criteria used. Section 5.0 recommends three vulnerability assessment and reasoning tools for inclusion in the NVT prototype. The surveyed vulnerability assessment technologies are summarized in Appendix A.

2.0 Survey of Vulnerability Assessment and Reasoning Tools

A trade survey of existing vulnerability assessment and reasoning tools was conducted to determine the scope of capabilities available for inclusion in the NVT prototype. The tools surveyed included:

- •Government-Off-The-Shelf (GOTS) tools, which were developed under Government contracts and are used for vulnerability assessment without additional tailoring as a "standard" capability.

•Commercial-Off-The-Shelf (COTS) products, which are sold for immediate application and maintained as commercial products, available on the open market.

• Research tools, which are still in the laboratory with varying phases of maturity.

Various methods were employed to identify the available vulnerability assessment and reasoning tools and to gather specific data on the tools. The methods and their results are summarized in Table 1, Survey Methods.

Table 1, Survey Methods

Method	Result
Internet search (various engines)	Voluminous and somewhat redundant data
Trade show attendance (MIS Institute/ISSA Open Systems Security Exposition, Orlando, FL (Date)	Clarification and vendor information on the most popular COTS products.
Trade Publications (Federal Computer Week, Internet Week, Network World, Information Security, Information Security Product News)	Multiple leads and vendor contact data, resulted in product literature, vendor discussion.
Canvas of Professional Associates	Additional Research Tools, unpublicized GOTS tools
Evaluation Copies (Risk Watch, Buddy System, Net Auditor)	Hands-on product assessment

The surveyed vulnerability assessment and reasoning tools with their NVT prototype relevant characteristics are summarized in Appendix A.

3.0 Tool Evaluation Criteria

The functional evaluation criteria used to select the vulnerability assessment and reasoning tools were selected to facilitate tools integration into the NVT prototype. The primary criteria were the operating system required by the tool, the capability of the tool to assess network environments, the data gathering methods used by the tool, and the risk types assessed by the tool. The surveyed tools varied greatly in their ability to meet the functional criteria. .

The vulnerability assessment and reasoning tools have to be able to run in the NVT prototype's operational environment consisting of the hardware platform and operating system. The required platforms were identified as one or more of the following operating systems; PC/DOS, Windows, MAC, UNIX, and WindowsNT.

For the NVT prototype to have the capability to assess the vulnerabilities and risks associated with a network or distributed system environment, the vulnerability assessment and reasoning tools need to be able to understand the vulnerabilities of an networked communications environment. In this evaluation, this criteria is termed 'Network Smart'. Initially this characteristic was defined as the capability to identify and assess network functions and components. Many of the COTS tools were originally developed for independent systems or systems with limited connectivity and were not considered "Network Smart". Further research indicated some of the tools could be configured to recognize basic network functions and components.

The NVT framework model is envisioned as interactively providing data to the vulnerability assessment and reasoning tools and synthesizing the result data received from the tools. Therefore, the methods by which the tools were designed to collect input data and the method and formats used to report result data were identified as key criteria.

The method of data collection was categorized as active or passive. The active method of data input:

- uses agent software for monitoring activity on the system,
- performs interactive traffic analysis for determining system structure,
- and may query identified nodes for connectivity, protocols, and users.

Active data gathering methods can be further decomposed into either active or active resident technologies. The active method is the predominant type used in the vulnerability assessment and reasoning tools. The active method gathers information only on the current state of the system being assessed, i.e., a single snap shot of the system being assessed. In the active resident method, the agent software remains persistent after the initial state is assessed and continues to monitor for additional activities and/or changes. This type of data gathering can provide ongoing analyses and some intrusion detection capabilities. This continuing assessment capability incurs a greater integration complexity for the NVT prototype.

The passive method of data input is:

- predominately user intensive
- characterized by system defined inputs configured during tool installation
- user inputs from questionnaire, and/or selectable inputs from a predefined data base.

Many of these tools were developed with an emphasis on the tool's reasoning and analysis capabilities and not on user friendly or automated data acquisition methods. While cumbersome to integrate into the interactive NVT framework, some of these tools are highly flexible and can accommodate diverse target system configurations.

Output characteristics of the tools were expressed in terms of:

- risk matrices identifying types of risks identified, e.g., system risk, component risk, operating system risk, etc,
    - annualized expected financial loss based on statistical probability of an identified vulnerability being exploited times the dollar value of the resource compromised,
- criticality of components defining the relative risk and the degree of risk that each component exposes the system to,
- compliance reports based on data gathered compared to a defined set of requirements,
- risk over time stated as a statistical probability of an occurrence during a given period of time.

None of the tools possessed configurable or tailorable output characteristics.

The last major functional criterion was the risk type analyzed by the vulnerability assessment and reasoning tool. While the supported operating systems and data gathering methods were definitive, concrete criteria, the risk types addressed by the tools varied greatly from identifying the risk in only general terms to identifying specific risks associated with individual functions to an infinite range of user defined risks. Having been developed for the commercial environment, many of the tools expressed risk in terms annualized financial loss expectancy.

The functional selection criteria for vulnerability assessment and reasoning tools are summarized in Table 2, Functional Criteria.

Table 2, Functional Criteria

Characteristic	Definition/Rationale
<u>Platform/Operating System:</u> This refers to the platform(s) and operating system(s) in which this tool can run.	The tool has to be able to run on the NVT prototype platform. Unique or additional environmental support software or hardware are more likely to result in later compatibility and integration problems when additional reasoning tools are incorporated into NVT.
<u>Product/Research:</u> The source and developmental status of the tool.	The availability of support for a tool is most likely from a commercial vendor. Additionally, the more mature a tool is the less likely modification will adversely affect the tool's integration into the NVT prototype.
<u>Risk Types Considered in the Analysis:</u> The types of risk that the tool evaluates.	The tools should include a comprehensive selection of risk types to be analyzed.
<u>Information Gathering Method:</u> The tool's data acquisition methods.	A tool with a passive data acquisition method is associated with system defined inputs, user questionnaire inputs, user selectable inputs from a generic data base, or any combination of these methods. An active data acquisition technology is associated with agent software monitoring activity on the system, performing traffic analysis for determining system structure and connectivity, querying identified nodes for connectivity, protocols, users, etc, or any combination of these methods. An active resident technology, after identifying the system parameters using any of the 'active' methods, remains persistent, continuing to monitor for additional activities and/or changes, and provides ongoing analyses. Finally, a tool may possess a combination of active, passive, and active resident technologies.
<u>Risk Metric Expressed in terms of:</u> The data output capability of the tool to provide relevant analysis data for the NVT prototype.	The output data of reasoning tools will be used by the NVT prototype for fusion with other tool's outputs into a cohesive, consolidated output. In order to provide a comprehensive view of the network under evaluation, the prototype requires as many different risk analyses types as possible

IW Smart: The capability of the tool to employ Information Warfare technologies and/or recognize offensive or defensive techniques.	If a reasoning tool possessed IW technologies its inclusion in the NVT prototype would be facilitated. Please explain what an IW technology is, this criteria isn't mentioned in the textual explanation.
Network Smart: The capability to assess network characteristics.	Many vulnerability assessment and reasoning tools were developed originally for independent monolithic systems or systems with limited connectivity; NOT for a network of systems.
Quantitative / Qualitative: The characterization of the tools output data.	The quantitative tool output can be expressed as a definitive value or a range of values. A qualitative output is expressed in subjective terms such as poor, good, better, best, highly vulnerable, less vulnerable, etc. In order to fuse the reasoning tool's output data, the prototype needs to understand the format and context of the output data.
Asset valuation: Whether the tool expresses risk in terms of financial loss/relative importance of components.	In order for the prototype to rank risks or vulnerabilities, the relative importance of each characteristic/component needs to be established.

4.0 Selection Process

A primary purpose of the NVT prototype is to demonstrate a framework model with the flexibility to integrate and interactively use existing vulnerability assessment and reasoning technologies. The existing COTS, GOTS, and research vulnerability assessment and reasoning tools were surveyed and their characteristics identified. In order to demonstrate the proof of concept within program restrictions, only a representative sample of tools is needed for inclusion in the NVT prototype. These selected tools have to represent the greatest diversity of characteristics while exposing the NVT program to the least amount of integration risks.

The primary consideration for selection was that the tools had to be able to run in the NVT prototype's operational environment without modification. Therefore the selected tools must be compatible with the selected operating system of the NVT prototype. Early in the selection process, WindowsNT was selected as the operating system of choice for the NVT prototype. Windows NT was selected due to its wide availability and acceptance in the target user community. This focused the survey process on the tools capable of running in the WindowsNT, Windows, and possibly the PC/DOS operating system environment. The vulnerability assessment and reasoning tools meeting the operating system requirements are identified in Table3, Tools' Operating System Requirements.

Table 3, Tools' Operating System Requirements

Product Name	Manufacturer information	Product/ Research	PC/DOS	PC/Windows	MAC	WindowsNT	UNIX
Norman Risk Analysis: The Buddy System	Norman Data Defense Systems, Inc. 3040 Williams Drive, 6th Floor Fairfax, Virginia 22031 (703) 573-8802 fax (703) 573-3919 http://www.norman.com/	product	√	√		√	
@ Risk	Palisade Corp, 31 Decker Rd., Newfield, NY 14867 800-432-7475 http://www.palisade.com/	product	√	√	√	√	
RAM Risk Assessment Model	National Security Agency POC Cpt Donald Buckshaw, R52	research		√		√	
PRISM Risk Analysis and Simulation for the PC (Note 1)	Palisade Corp, 31 Decker Rd., Newfield, NY 14867 800-432-7475 http://www.palisade.com/	product		√	√	√	
ANSSR	Mitre Corp Bedford, MA POC: Mr. Fred Chase fnc@mitre.org	research	(Note 2)				
Secure Detector	ODS Networks Inc. Richardson, TX 75024 http://www.ods.com/	product		√		√	
Kane Security Analyst	Intrusion Detection, Inc http://www.intrusion.com/ IDI acquired by Security Dynamics, Bedford, MA http://205.181.76.22/	product		√		√	
ISS Scanner Toolset	Internet Security Systems Atlanta, GA http://www.iss.net/	product		√		√	√
ISS Internet Scanner	Internet Security Systems Atlanta, GA http://www.iss.net/	product		√		√	√
WebTrends Security Analyzer (Previously named Asmodeus)	WebTrends Corporation free v2.0 Beta from http://www.webtrends.com/wss/	research/ development		√		√	

Note 1 PRISM has been incorporated into @Risk
Note 2 Smalltalk compatible platforms

A design goal of The NVT analysis framework is support for multiple and varied vulnerability assessment and reasoning tools. To demonstrate this design goal the NVT prototype should include multiple vulnerability assessment and reasoning tools with varied major tool characteristics. Within program time and cost constraints only two, or possibly three, vulnerability assessment and reasoning tools can be incorporated into the NVT prototype.

The selected tools should represent the largest diversity within the major characteristics of data

acquisition, output format, and risk types. The selected tools are representative both of the active and passive data acquisition technologies. The active resident data gathering tools are not included because of the complexity associated with assimilating the continuous output data within the NVT prototype. Program constraints dictate that the NVT prototype demonstrate the ability to synthesize the outputs from multiple vulnerability assessment and reasoning tools as a primary objective. Resolving the complexities of continuous data output from a single tool is beyond the present scope of the program. Finally, it is desirable that the selected vulnerability assessment and reasoning tools be capable of analyzing a variety of risk types.

The selection process criteria eliminated from further consideration, those vulnerability assessment and reasoning tools which were not compatible with the WindowsNT operating system and those with active resident data gathering technologies. The remaining tools were evaluated as to their advantages and disadvantages for inclusion in the NVT prototype. This subset of candidate vulnerability assessment and reasoning tools is summarized in Table 4, Tools' Advantages and Disadvantages, enumerating the advantages and disadvantages of each tool.

Table 4, Tools' Advantages and Disadvantages

Product	Platform/ OS	Information Gathering Method	Advantages	Disadvantages
Buddy System	PC/DOS, PC/ Windows	survey	analysis includes networks, stable COTS product,	no risks analyzed only expressed in terms of possible annual loss single level survey input
"@ Risk	PC/DOS, Windows, MAC	User Defined Algorithm	data gathering and risk types analyzed flexible but complex through user defined algorithms	no risks analyzed only expressed in terms of possible non dollar loss does not analyze networks
RAM Risk Assessment Model	PC/Windows	Combination active and passive; partial survey	data gathering through a combination of active and passive methods denial of service risk expressed over time available from another government agency	single type of risk analyzed does not actively identify network vulnerabilities
PRISM Risk Analysis and Simulation for the PC	PC/Windows, MAC	User Defined Algorithm	accommodates simulations of different system configurations	risk expressed only in non dollars does not analyze network vulnerabilities
ANSSR	Smalltalk compatible platforms	survey, Q&A	multiple risk types analyzed multi-level passive input method IW cognizant analyzes network vulnerabilities	research product - possibly limited support
ISS Internet Scanner	WindowsNT, Unix	active, graphical	analyzes network vulnerabilities active data gathering multiple risk types analyzed	risk expressed in compliance report

Only the last entry in the above table, the ISS Internet Scanner, uses an active single state data gathering technology exclusively. All the other gathering vulnerability assessment and reasoning tools have passive data gathering methods or require the use of a combination of passive and active methods.

5.0 Recommendation

A comparison of the functional evaluation criteria required for the NVT demonstration versus those characteristics identified as being available in the seven remaining vulnerability assessment and reasoning tools is shown in Table 5, Tools' Operational Characteristics.

Table 5, Tools' Operational Characteristics

Vulnerability Assessment Tool	WindowsNT Operating System	Active Data Gathering Method	Passive Data Gathering Method	Network Smart	Number of Risk Types Assessed
Buddy System	Yes	No	Yes	Yes	0
"@ Risk	Yes	No	Yes	No	0
RAM Risk Assessment Model	Yes	Yes	Yes	No	1
PRISM Risk Analysis and Simulation for the PC	Yes	No	Yes	No	0
ANSSR	Yes	No	Yes	Yes	multiple
ISS Internet Scanner	Yes	Yes	No	Yes	multiple

Only the ISS Internet Scanner employs a totally active data acquisition method and is considered network smart. Of the other five vulnerability assessment and reasoning tools (Buddy System, "@ Risk, RAM Risk Assessment Model, PRISM Risk Analysis and Simulation for the PC, and ANSSR) identified as having passive data gathering capabilities, RAM Risk Assessment Model, and ANSSR assess specific risk types. ANSSR, RAM Risk Assessment Model, and ISS Internet Scanner are recommended for inclusion in the NVT prototype. These three vulnerability assessment and reasoning tools meet the NVT prototype requirements and provide the greatest diversity of functional capabilities as shown in Table 6, Recommended Tools' Capabilities summary. The final selection of the product used should be made with the endorsement and involvement of the Program Office.

Table 6, Recommended Tools' Capabilities Summary

Recommended Candidate	Functional Capabilities
ANSSR (Analysis of Networked Systems Security Risks - Mitre Corporation	Passive data gathering - Model structure - Survey based data gathering - Network aware Risk Type - Single Occurrence of Loss
RAM (Risk Assessment Model) - NSA	Passive data gathering - Event tree - Prioritized attack list Risk Type - Mathematical model - Multiple risks / services - Event based over time Extensible to Risk Type - Comparison of effectiveness of different designs - Not limited to computers/networks - Optimization of system / cost benefit analysis
ISS (Internet Security Systems) Internet Scanner - Internet Security Systems Corporation	Active data gathering - Scans network for hosts, servers, firewalls, and routers - Assesses security and policy compliance of networks, operating systems, and software applications Risk Type - Computer Network Compliance Report (snapshot in time)

Appendix A - Vulnerability Assessment Technologies Summary

The vulnerability assessment and reasoning tools surveyed are summarized in Table A1, Vulnerability Assessment Technologies Summary. The selection WindowsNT as the NVT prototype's operating system restricted the potential tools surveyed to those capable of executing within a WindowsNT environment. In addition to identifying the vulnerability assessment and reasoning tools surveyed, Table A1 summarizes each tool's applicable characteristics. Those characteristics are:

- **Product/ Research -** Product: The tool is available as a COTS product. Research: The tool is available from an organization which developed the tool as a research program and the organization has not offered the tool as a commercial product.

- **Platform/ OS -** This identifies the operating system(s) on which the tool was originally developed and intended to execute.

- **Risk Types considered in analysis -** This identifies which risks the tool analyzes.

- **Information Gathering Method -** This is the method which the tool uses to collect the data necessary to analyze its stated risk types.

1. Survey: A user filled out questionaire(s) for the system being analyzed.
2. Q&A: A user answering questions in an interactive session with the tool.
3. User Defined Algorithm: The method of data gathering varies depending on the user's selection of the tool's capabilities and the degree of granularity desired.
4. Passive, Active, and Active resident: The tool gathers significant portion of data through automated techniques from physical connections to the system being analyzed.
5. Graphical: Interactive user input via a graphical representation.

- **Risk Metric Expressed in terms of -** How the tool defines output of its analysis.

- **IW Smart -** Where or not the tool has the capability to analyze Information Warfare vulnerabilities.

- **Network Smart -** Where or not the tool recognizes and analyzes network vulnerabilities.

- **Quantitative/ qualitative -** How the tool presents the degree of risk associated with each identified vulnerability. Quantitative: e.g., number of vulnerabilities associated with each network node. Qualitative: e.g., risk ranking based on a defined scale.

- **Asset valuation -** Where or not the tool is capable of associating an asset valuation with each vulnerability/risk.

Table A1, Vulnerability Assessment Technologies Summary

Product Name	**Manufacturer information**	**Product/ Research**	**Platform/ OS**	**Risk Types considered in analysis**	**Information Gathering Method**	**Risk Metric Expressed in terms of**	**IW Smart**	**Network Smart**	**Quantitative / qualitative**	**Asset valuation**
IST/RAMP International Security Technology Risk Analysis Management Program	International Security Technology	product	IBM mainframe w/PC	delay, physical, damage, fraud, unauthorized disclosure	survey, Q&A	single loss occurrence	no	no	Quantitative	partial
BDSS Bayesian Decision Support System	A SYS T Inc.	product	PC/DOS	Asset loss	survey, Q&A	Annualized loss exposure	no	N/A	both	yes
Criti Calc	International Security Technology	product	PC/DOS	data destruction, unavailability	Q&A	Annualized loss exposure	no	no	both	yes
CRAMM CCTA Risk Analysis and Management Methodology	BIS Applied Systems Limited UK	product	PC/DOS	disclosure modification, denial of service, destruction	survey, Q&A	risk ranking	no	no	Quantitative	yes
MicroSecure Self Assessment	Boden Associates	product not supported	PC/DOS	disclosure modification, denial of service, destruction	survey	risk no metrics	no	no	Qualitative	no
GRA/SYS	Small Business Administration Nander & Brown	GFE product	PC/DOS	loss	survey	risk ranking	no	no	Qualitative	no
ALRAM Automated Livermore Risk Analysis Methodology	Expert-Ease Systems	product	PC/DOS	N/A	survey	risk ranking	N/A	N/A	Quantitative	yes
Control It	Jerry Fitzgerald and Assoc.	Product	PC/DOS	N/A	Q&A	risk ranking	no	partial	Quantitative	no
RA/SYS	Small Business Administration Nander & Brown	GFE product	PC/DOS	N/A	survey	Risk Ranking & Expected Loss	N/A	N/A	Quantitative	yes
Rank It	Jerry Fitzgerald and Assoc.	product	PC/DOS	N/A	Q&A	Risk Ranking	no	partial	Quantitative	no
RiskPAC	Computer Security Associates	product	PC/DOS	N/A	survey	Annualized loss exposure, dollar and nondollar	N/A	N/A	both	yes

Table A1, Vulnerability Assessment Technologies Summary - Continued

Product Name	Manufacturer information	Product/ Research	Platform/ OS	Risk Types considered in analysis	Information Gathering Method	Risk Metric Expressed in terms of	IW Smart	Network Smart	Quantitative / qualitative	Asset valuation
RiskWatch	Expert Systems Software	product	PC/DOS	N/A	survey, Q&A	Annualized Loss Exposure	partial	yes	both	yes
SOS Security Online System	Entellus Technology Group	product	PC/DOS	N/A	survey	Annualized Loss Exposure	partial	partial	both	yes
ARES Automated Risk Evaluation System	AF contractor for AFCSC/SR	research	PC/DOS	OPSEC	survey	Risk listing	no	no	Quantitative	yes
Janber	Eagon, McAllister Associates, Inc	Product unsupported	PC/DOS	OPSEC	survey, Q&A	risk ranking	no	no	Quantitative	no
MARION	Cooper & Lybrand UK	product	PC/DOS	OPSEC	survey	scaled risk	no	no	Quantitative	no
MINIRISK	Small Business Administration Nander & Brown	GFE product	PC/DOS	OPSEC	survey	scaled risk	no	no	Qualitative	no
LLAVA Los Alamos Vulnerability and Risk Assessment	Barranca Inc	product	PC/DOS	OPSEC LAN, PC	survey, Q&A	scaled risk	some	yes	Qualitative	N/A
CONMAT Control Matrix	Small Business Administration Nander & Brown	GFE product	PC/DOS	single machine application	survey	risk ranking	no	no	Qualitative	no
RiskCALC	Hoffman Business Associates	product	PC/DOS	loss	survey	Annualized loss exposure, dollar and nondollar	no	no	Quantitative	yes
Buddy System	Norman Data Systems	Product	PC/DOS, PC/ Windows	N/A	survey	Annualized loss exposure	N/A	yes	Qualitative	yes
"@ Risk	Palisade Corp, Newfield	Product	PC/DOS, Windows, MAC	User Defined Algorithm	User Defined Algorithm	Expected Loss (non-dollar)	N/A	N/A	Quantitative	N/A
RAM Risk Assessment Model	NSA	research	PC/ Windows	denial of "service"	partial survey	risk over time	no	no	both	no

Table A1, Vulnerability Assessment Technologies Summary - Continued

Product Name	**Manufacturer information**	**Product/ Research**	**Platform/ OS**	**Risk Types considered in analysis**	**Information Gathering Method**	**Risk Metric Expressed in terms of**	**IW Smart**	**Network Smart**	**Quantitative / qualitative**	**Asset valuation**
PRISM Risk Analysis and Simulation for the PC	Palisade Corp, Newfield	product	PC/ Windows, MAC	User Defined Algorithm	User Defined Algorithm	Expected Loss (non-dollar)	no	no	Quantitative	N/A
ANSSR	Mitre Corp	research	Smalltalk compatible platforms	Network, unauthorized disclosure, denial of service	survey, Q&A	single loss occurrence	partial	yes	Quantitative	yes
VISART Risk Analysis, Confidentiality & Extending Expected Value	NSA	research	unk	multiple risks	unk	aggregate risks for protecting critical assets	unk	unk	both	unk
Secure Detector	ODS Networks Inc.	product	Windows NT	intrusion detection	active resident, partial graphical	compliance reports	no	yes	Quantitative	no
Kane Security Analyst	Intrusion Detection, Inc IDI acquired by Security Dynamics	product	Windows NT	unauthorized access, denial of service	active resident, graphical	risk ranking	no	partial	both	no
ISS Scanner Toolset	Internet Security Systems	product	Windows NT, Unix	anomaly detection	active, partial resident; graphical	compliance reports	no	yes	Quantitative	no
ISS Internet Scanner	Internet Security Systems	Product	Windows NT, Unix	Network, o/s, s/w	active, graphical	compliance reports	N/A	yes	Qualitative	no
WebTrends Security Analyzer (formally Asmodeus)	WebTrends Corporation	product - beta	Windows NT	scan IP ports on multiple servers for available services and ipotential weaknesses	active, resident	user defined response	no	yes	Quantitative	no
netformX	netformX, Inc.	product	Windows, NT	network visualization	active	reports	no	no	Qualitative	no
Analyser	Netman Development Group at Curtin University of Technology, Perth, Western Australia	academic release	Unix	configuration optimizer	passive, input from other tools	reports	no	no	Qualitative	no
Argus	Software Engineering Institute, Carnegia Mellon University	public domain generic IP network transaction auditing tool	Unix	audit data reduction	passive, audit data, reading network datagrams	network traffic status records	no	partial	Quantitative	no

System Vulnerability Analysis with the Network Visualization Tool (NVT)[1]

Ronda R. Henning[2]
Kevin L. Fox, Ph.D.[2]

Next generation information systems and infrastructures apply the concept of acceptable risk to vulnerability assessment and coalition information sharing. The security features of the system architecture provide sufficient protection for the mission and data processed. In previous generations of systems, a risk adverse vulnerability posture dictated custom hardware and software solutions and minimal coalition data interchange. There are few system architecture design tools available to analyze architecture alternatives among security risk, system performance, and mission functionality while accommodating budgetary constraints. Current generation risk analysis tools provide single vendor monolithic solutions that address a particular aspect of risk, but are not easily expanded to address emerging technologies and their vulnerabilities.

For the past two years, Harris Corporation has been conducting research for the U.S. Air Force Research Laboratory under the Network Vulnerability Tool (NVT) Study. The Network Vulnerability Tool concept uses a single topological model to support the information needs of multiple vulnerability analysis tools through a knowledge solicitation and translation framework. As part of this effort, existing COTS, GOTS, and research laboratory vulnerability assessment tools were surveyed, and a representative sample of tools was selected for inclusion in the NVT prototype. The prototype integrates and interactively applies multiple existing vulnerability assessment technologies, to produce a cohesive, combined vulnerability/risk assessment. This helps the analyst define an acceptable risk posture for a deployed or preliminary system design. NVT defines a preliminary vulnerability assessment environment, consolidating multi-source output into a cohesive visual vulnerability assessment capability.

This functionality can be used as a tool to:

- identify vulnerabilities in systems early in the development process,
- baseline the security configuration of a developed system,
- trace security configuration changes over the system lifecycle, and
- facilitate "defense in depth" security perimeter definition activities.

This presentation describes the NVT development effort, and some preliminary results from using the tool.

[1] This research has been entirely funded under the Network Visualization Tool (NVT) program for U.S. AFRL/IFGB, contract #F30602-96-C-0289.
[2] Harris Information Systems Division, P.O. Box 98000, 150 S. Wickham Road, Melbourne, FL 32902.

EXHIBIT 2

NVT Prototype Design Notes

NVT DEMONSTRATION

- Test/demonstration network for NVT prototype will be a subset of HISD's network. (Decision made a TIM #5.)

NVT LAB ENVIRONMENT

- Set up network for NVT lab in W3/2607
- Upgraded Lab to Visual Studio 6.0
- Visual Basic 6.0
- Purchase order placed for VisualWorks 3.0 ?

ANSSR

- After considerable effort, resolved Smalltalk/ANSSR issues;
    - ANSSR was written in ObjectWorks Smalltalk version 4.1
        - Encountered challenges in integrating this tool under Visual Smalltalk due to Smalltalk compatibility issues
        - Solved most compatibility issues by using VisualWorks Smalltalk, a readily available successor to ObjectWorks
        - ANSSR has now been successfully built under VisualWorks 3.0
- Testing is ongoing, but outlook for use of ANSSR under VisualWorks Smalltalk 3.0 is promising
- Output from ANSSR is a Vulnerabilities Report (ascii text file) which contains
    - Summary information
    - For each component in the network, a list of vulnerabilities and a # (rating or ranking?)

ISS INTERNET SCANNER

- Could be used as one way to resolve incomplete data problem. Used to ping network node to discover information about the node.

RAM

- The CRADA with NSA through which we would obtain a copy of RAM is still unsigned, tied up in NSA legal.
- The delay in obtaining a copy of RAM from NSA is impacting the schedule for the development of the NVT prototype. By the end of December, we should have completed the acquisition and initial study of each vulnerability assessment tool, as well as have designed our initial prototype. Without a copy of RAM, we cannot complete an initial study of integration issues involved with the tool, or complete the initial design.
- Therefore, if the CRADA is not completed soon, we will need to resort to Plan B, which is to use the Harris STAT vulnerability DB.

NVT PROTOTYPE DESIGN

- OpenView D.01 (which is currently installed in NVT Lab, purchased in February and received in March 1998) supports Visual Basic 3.0. OpenView D.03 (most recent release) supports Visual Basic 4.0 (and 3.0). But we have Visual Basic 6.0, and thus have a compatibility problem. Because of this, we will not be able to use some HP

EXHIBIT 3

Visual ____ tools, which would have made it easier to integrate with Visual Studio 6.0.

Vulnerability Architecture

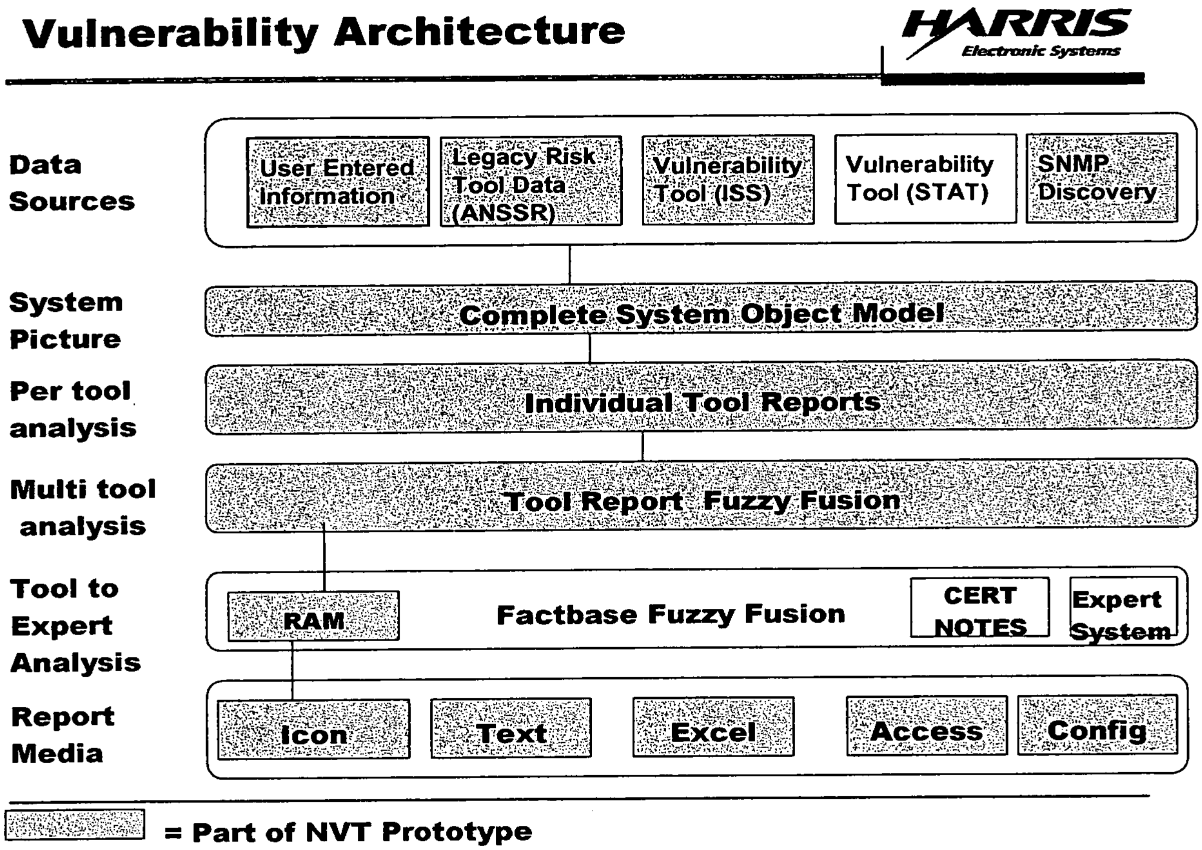


EXHIBIT 4

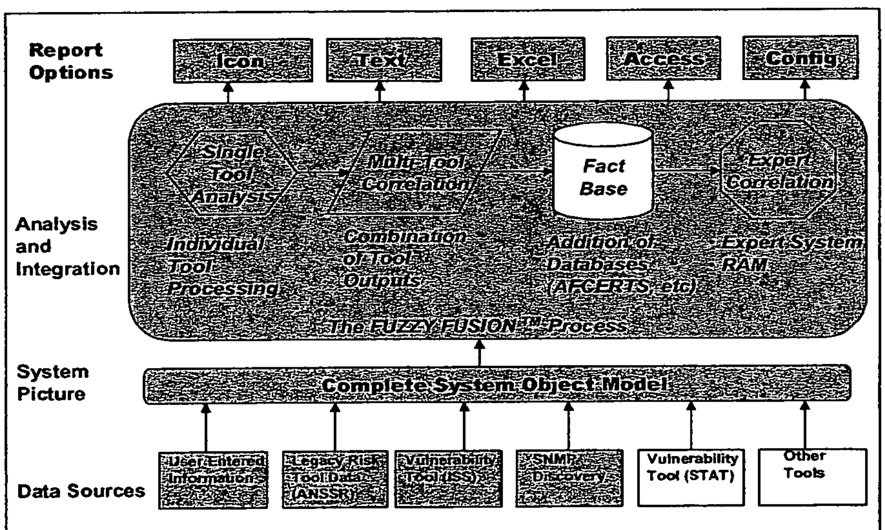
R.R. Henning

Version 1.0

Network Visualization Tool (NVT) Program Patent Disclosures

During the development of the NVT proof of concept prototype, three unique, distinct ideas have been generated that merit further patent investigation:

1. The NVT overall architecture represented in Figure 1. The NVT architecture is unique in its integration of multiple different risk assessment tools and network discovery agents. To our knowledge, no existing vulnerability analysis architecture:
   - allows integration of alternate assessment tools
   - uses input from a network management SNMP automatic discovery as an alternate data source
   - derives a more comprehensive system object model from the aggregate of the risk assessment tool inputs
   - de-couples processing, ingest, and output into discrete components
   - was designed to accommodate advanced technologies and integration of additional capabilities.



NVT Technical Architecture

2. Fuzzy Fusion™ is a unique, Harris developed reasoning architecture that combines the use of data correlation, fuzzy logic, expert system, and knowledge-based reasoning to provide a more robust conclusion based on the discrete data facts at hand.
3. Object Filters provide a unique Object-Oriented API that allows ready incorporation of new tools and technologies. The Object Filtering approach supports isolation of ingest, processing, and reporting mechanisms. It also facilitates the provision of alternate report formats.

EXHIBIT 5

System Vulnerability Analysis with the Network Visualization Tool (NVT)[1]

Ronda R. Henning[2]
Kevin L. Fox, Ph.D.[3]

Harris Corporation
Information Systems Division
P.O. Box 98000
Melbourne, FL USA 32902-9800

Summary: For the past 2 years, Harris Corporation has been conducting research for the Air Force Research Laboratory under the Network Visualization Tool (NVT) Program. The NVT concept defines a knowledge solicitation and translation framework for risk assessment. This framework incorporates a graphical description of a network topology, a central repository of modeling data, and report consolidation from multiple risk/vulnerability assessment tools into a single vulnerability assessment. Results are presented to a system user through a comprehensible, graphical interface. The goal of this effort is to investigate the feasibility of developing such a framework for a graphical risk analysis environment that can accommodate both existing and new risk analysis techniques.

The result of the NVT Program is an initial vulnerability visualization and assessment environment, consolidating multi-source output into a cohesive capability with an open, a standards-based architecture. The initial NVT proof-of-concept prototype has been completed. This paper describes the NVT architecture, its components, important architecture features, benefits of the NVT approach, and potential future enhancements.

I. INTRODUCTION

Next generation information systems and infrastructures apply the concept of acceptable risk to vulnerability assessment and coalition information sharing. In this environment, the security features of the system architecture are considered sufficient protection for the mission and any supporting data processed. In previous generations of systems, a risk adverse vulnerability posture dictated custom hardware and software solutions and minimal coalition data interchange. Today, the rapid evolution of technology and the proliferation of computing power mandate the use of commodity Commercial-Off-The-Shelf (COTS) hardware and software components for cost effective solutions. This strong dependence on COTS implies that commercial grade security mechanisms are sufficient for most applications. Security architectures, therefore, must be structured to support building security architectures with relatively weak COTS components. Higher assurance security components are placed at community or information boundaries, forming an enclave-based security architecture that implements a defense-in-depth approach to information assurance.

There are few system architecture design tools available to analyze architecture alternatives. Security risk, system performance, and mission functionality must be balanced while accommodating budgetary constraints. Current generation risk analysis tools usually provide single vendor solutions that address a particular aspects of risk, but are not easily expanded to address emerging technologies and their vulnerabilities. These tools tend to fall into one of three categories:

1. Tools using documented vulnerability databases and possibly repairing known vulnerabilities. Tools of this type are vendor-dependent for database updates, either through new product versions or by a subscription service. Examples of tools in this category are Internet Security System's (ISS) Security Scanner and Network Associates Inc.'s CyberCop.
2. Monolithic tools using various parameters to calculate a risk indicator. These tools are difficult to maintain and harder to keep current in the rapidly evolving threat and technology environment. An example of this tool category is the Los Alamas Vulnerability Assessment Tool (LAVA).
3. Tools examining a particular aspect of the system, such as the operating system or database management system, but ignoring other aspects of the system. SATAN, for example, analyzes operating system vulnerabilities but ignores infrastructure components such as routers and switches.

None of these tools implement an aggregate security snapshot approach to the system, with a "drill down" or layered approach to facilitate addressing risk at various layers (network, platform, database, etc.) of the system. They provide little assistance to system designers when analyzing alternatives among security risk, system performance and mission functionality, instead providing a "risk solution" addressing the particular aspect of risk

---

[1] This research has been entirely funded under the Network Visualization Tool (NVT) program for U.S. AFRL/IFGB, contract #F30602-96-C-0289. U.S. Government Publication Release Authority: Dwayne Allain.

[2] Telephone: (407) 984-6009. E-mail: rhenning@harris.com

[3] Telephone: (407) 984-6011. E-mail: kfox@harris.com.

EXHIBIT 6

that a given tool was designed to address. To develop a comprehensive risk picture, a tool user would have to become proficient in the use of several tools, and manually correlate the resulting outputs.

Risk analysis is the assessment of the potential system vulnerabilities that may give rise to a security violation. An essential criterion for successful risk analysis is complete and accurate data for the generation of the system models used by the analysis tools. Most of the current risk analysis tools rely on surveys filled out by users, system operations personnel, and analysts to acquire the data for development of the system model. Alternatively, active network scanning may be used to test various vulnerabilities against system components. Textual or survey-based knowledge solicitation techniques are labor intensive and potentially tedious for the analyst. Many of the existing tools reuse the same information to analyze different aspects of the system security.

A centralized repository of system modeling data could provide a basis for shared inputs among existing tools. This repository could generate data sets for use by risk analysis tools, allowing multiple tools to be executed against the same system without separate input activities, and reducing the possibility of operator error. The use of multiple risk tools for backend analysis would allow various aspects of the system to be analyzed without the cost of developing one tool to perform all types of analysis. Integration of the information and the resulting informed assessments made available through multiple tool analyses could produce a more robust and accurate picture of a system's vulnerability posture. By providing an easier framework for alternative evaluation and comparison, these results could facilitate more informed system design decisions.

The Network Visualization Tool (NVT) Program explored the feasibility of defining a shared data repository for risk assessment information. The results of our research included a vulnerability analysis tool framework, a working proof of concept of the architecture, and an innovative application of data fusion technologies to the risk analysis environment. This paper describes the progress and results of the NVT Program.

II. SYSTEM OVERVIEW

Under the Network Visualization Tool program, Harris Corporation defined and developed an innovative and unique vulnerability assessment framework. This framework, the NVT system architecture, can accommodate changes to the threat and the technology environments and preserve the results from current risk analysis tools. The goal of this effort is to research, develop, test, and demonstrate an engineering prototype for a system vulnerability assessment framework that helps system architects identify security vulnerabilities and develop cost-effective countermeasures.

NVT provides a flexible, extensible, and maintainable architecture solution. The NVT prototype isolates factual information about a system from the reporting and processing capabilities of individual vulnerability assessment tools. No single vulnerability assessment tool can adequately address all components of a comprehensive system architecture. A monolithic assessment system is difficult to evolve with the dynamic nature of threat and technology. NVT allows multiple tools to share data and provides a concise, understandable report to the system user. Our objective was to develop a prototype system security engineering tool that:

- Functions as a design tool to identify vulnerabilities in an architecture before the architecture is built and help enforce good security design principles
- "Snapshots" a system and its vulnerabilities, and compares how risk evolves over the system life cycle
- Applies static vulnerability databases from a variety of sources
- Applies legacy risk analysis tools and threat models
- Correlates information from various risk models/tools into a more comprehensible picture of the system's vulnerabilities
- Allows what-if analysis to facilitate comparative analysis among security, functionality, performance, and availability
- Provides an easy to use capability to specify the security relevant characteristics of a system design
- Our vision of a system security engineering tool that facilitates system vulnerability assessment incorporates a single, graphical representation of a system. This system representation is provided to multiple risk/vulnerability assessment tools and vulnerability data or knowledge bases, resulting in a single source, consolidated input system model for multiple tools. The NVT prototype integrates and interactively applies multiple existing risk assessment technologies. A Fuzzy Expert System applies the unique correlation technology of ***FuzzyFusion***™ to combine the results from the various tools into a single, clear, cohesive vulnerability assessment report. The concept is illustrated in Figure 1.

The NVT prototype is implemented on an Intel Pentium PC platform running Windows NT. This platform was selected as a low cost solution supporting a large variety of assessment tools. The initial tool suite employs a number of COTS/GOTS capabilities including:

- HP OpenView, for network automatic discovery or manual network modeling.
- ANSSR, a Government-Off-The-Shelf (GOTS) network system analysis tool developed by MITRE.
- RAM, NSA's risk assessment methodology, implemented in the DPL-F decision support programming language.
- Internet Security Systems Internet Scanner, a scanning vulnerability tool suite.

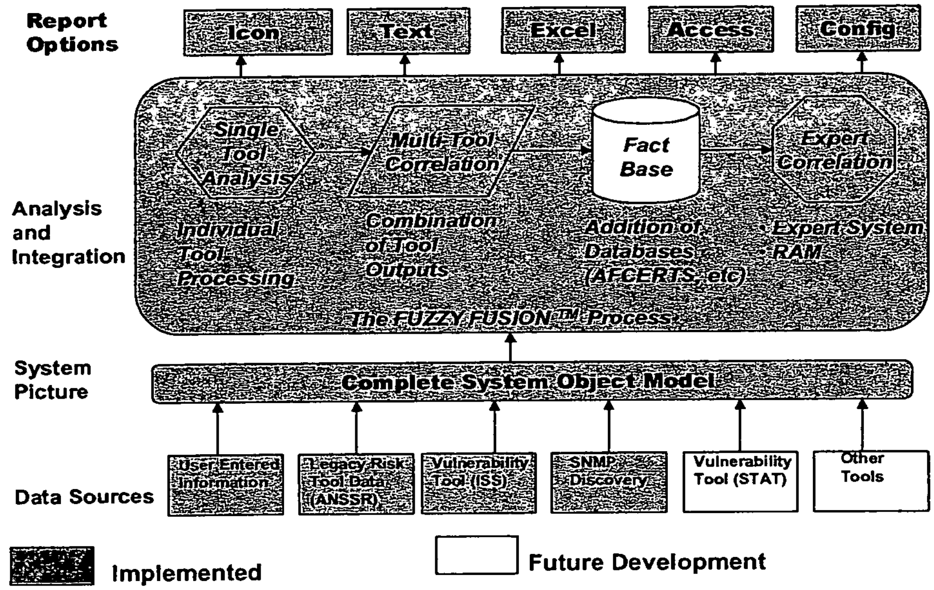


Figure 1. – The NVT Vulnerability Assessment Tool Architecture Concept.

II.1 System Architecture Data Entry

NVT is based on the concept of a knowledge solicitation framework that incorporates a graphical description of a network topology. This topology is used for capture of network attributes, and is subsequently analyzed for security vulnerabilities. The knowledge solicitation portion of NVT applies modern network discovery capabilities and a graphical user interface. This improves the accuracy of the network model, provides a common network description for multiple risk analysis reasoning engines, and enhances the productivity of the system security analyst.

The NVT prototype automatically maps an existing network, or can be used for the manual entry of a network design. The prototype uses HP OpenView to graphically depict a network topology. As illustrated in Figure 2, once it has been given the IP address of the default router for the network, NVT, through the use of OpenView, can search for computers and other devices attached to the network. It performs an active search, pinging possible IP addresses on the network, and adding whatever response information it receives to its network map. NVT also provides, through OpenView, a manual method to draw a proposed network with a graphical user interface that supports drag and drop, as illustrated in Figure 3.

Through this interface, a System Security Engineer can rapidly define a given system architecture, including the security critical information. For example:

- A user can apply the manual entry capability to consider alternative designs as part of a trade study.
- A user may edit the properties of each node, providing additional details as required to provide complete logical network planning.
- A user can also represent an entire network on a map by using a subnetwork icon. A detailed map of the subnetwork can be linked to this icon and displayed by double clicking on the icon.

Once the system description has been completed, the NVT prototype represents and stores the description in an object/class hierarchy. This single topological model supports the information needs of multiple vulnerability assessment tools, as well as the ***FuzzyFusion™*** of their results into a cohesive risk assessment. NVT translates this system representation into the appropriate format for each of the assessment tools employed. This single object representation of the system simplifies the use of multiple tools, eliminating redundant data entry. It also provides the foundation for addressing the problem of incomplete data for a given vulnerability assessment tool, and for future knowledge negotiation capabilities to correct data inconsistencies.

II.2 Risk Analysis Tool Selection

Under the NVT Program, Harris surveyed current COTS, GOTS and research vulnerability assessment and reasoning tools to determine their capabilities and availability. Tools were categorized by the types of vulnerabilities assessed, and their functional characteristics. Each tool was further evaluated on its data acquisition and output formats to determine how the information can be applied in the NVT engineering prototype implementation. The primary criteria were the operating system required by the tool, the capability of the tool to assess network environments, the data gathering methods used by the tool, and the risk types assessed by the tool. The vulnerability assessment and reasoning tools selected had to be able to execute in the NVT prototype's operational environment (a PC with Windows NT).

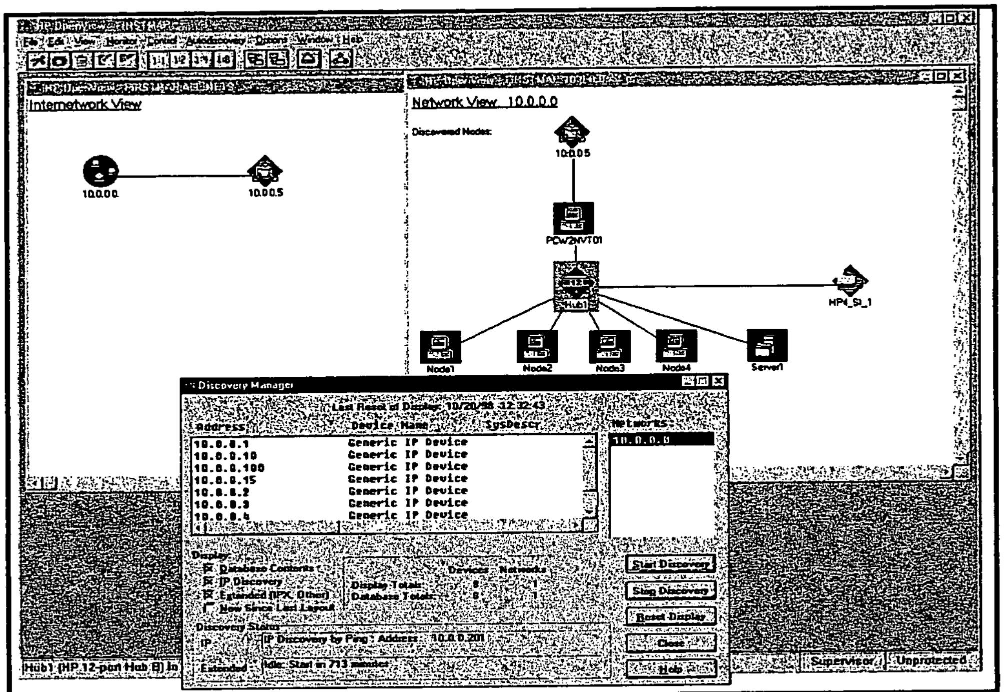


Figure 2. HP OpenView's Network Discovery Tools enable NVT users to map an Existing Network for Further Security Analysis

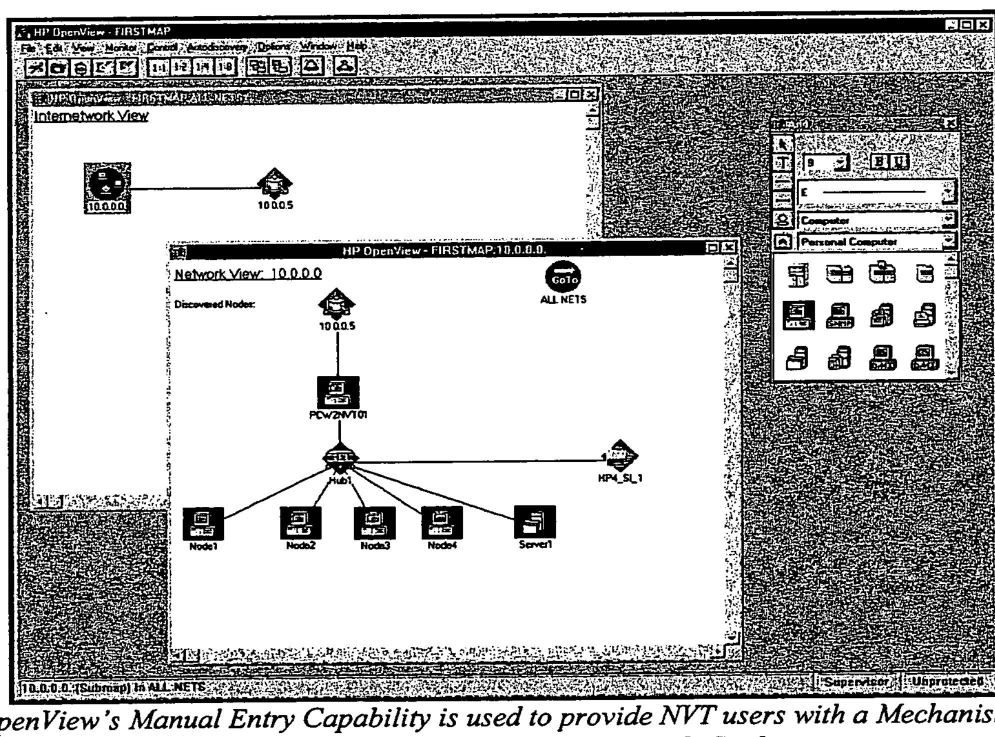


Figure 3. OpenView's Manual Entry Capability is used to provide NVT users with a Mechanism to Consider Alternative Designs as Part of a Trade Study

A primary purpose of the NVT prototype was the demonstration of a framework with the flexibility to integrate and interactively use multiple existing vulnerability assessment and reasoning technologies. In order to demonstrate the proof of concept of integrating and interactively using multiple existing vulnerability assessment and reasoning technologies within program restrictions, a representative sample of tools was selected for inclusion in NVT. As a result of the tool survey, ANSSR, RAM, and ISS Internet Scanner were selected for inclusion in NVT. These three tools met the project requirements and provided the greatest diversity of func-

tional capabilities, as shown in Table 1, The Selected Tools' Capabilities Summary. The selected tools represented the greatest diversity of reasoning characteristics with the lowest number of expected integration risks.

The MITRE Corporation's Analysis of Networked Systems Security Risks (ANSSR) prototype is a risk analysis tool which simulates attacks on information systems and communications between them that result in unauthorized disclosure of sensitive information. These simulated attacks, or threat scenarios, can be initiated by different types of attackers, including insider threats as well as those coming from outside an intranetwork . ANSSR compares the risk-reducing effects of different sets of safeguards in light of a given security concept of operations. Safeguards include computer security (COMPUSEC) features and assurances, communications security (COMSEC) controls, emanations protection, physical security, and procedural controls. ANSSR explicitly analyzes risks due to networking. ANSSR 2.2 includes simulated passive and active wiretap attacks as well as attacks in which an attacker, logged on at one system, exploits that system's connectivity to other systems to attack them. ANSSR can also be applied to a stand-alone system. An analyst can enter or reuse a baseline system description, then ask ANSSR to develop all possible scenarios against the baseline system. Single-scenario risks are aggregated into a bottom-line risk of all possible scenarios. ANSSR is intended primarily for use during the requirements definition phase, but can also be used to guide the risk analysis performed to support accreditation.

Internet Security Systems' (ISS) Internet Scanner is a fast, comprehensive and proactive Windows NT and UNIX network security scanner. It is a vulnerability assessment product that analyzes the security of devices on an enterprise-wide network. It has 30 predefined reports that are used to collect the information needed to make security policy decisions. Internet Scanner performs a variety of vulnerability detection, ranging from information-gleaning exercises to finding vulnerabilities. It finds vulnerabilities much as an intruder would – by examining a network's devices, services, and interrelationships. Internet Scanner provides detailed information about all vulnerabilities detected, including the vulnerable host, description, and corrective actions. It also provides illustrated management and trends analysis reports. Internet Scanner can be used on all TCP/IP-based networks – networks connected to the Internet as well as stand-alone networks and machines.

NSA's Risk Analysis Model (RAM) is a methodology to help balance an acceptable risk profile. RAM is a flexible methodology, utilizing event trees and a functional probabilistic decomposition of a problem. It moves the risk assessment process from a qualitative discipline to quantitative discipline. Users identify the probabilities of various events, and RAM aggregates the probabilities, as well as addressing vulnerabilities over time. RAM is an analytic methodology that enables analysis of risk for decision trade-offs. It allows for sensitivity analysis, and identifies the weakest links of a system. RAM has been incorporated into a COTS tool, the DPL-f programming language for decision support, developed by Applied Decision Analysis LLC, a wholly owned subsidiary of Price Waterhouse Coopers Ltd.

DPL (Decision Programming Language) is a decision support software package that facilitates the modeling of complex decisions. It allows a user to incorporate uncertainty and flexibility into the decision process. DPL provides a graphical interface for building a model, and performs a variety of analyses on the model. DPL-f contains all of the functionality built into DPL. In addition, DPL-f provides a graphic interface for fault tree construction. This feature allows the modeler to create fault trees and incorporate them into DPL models. DPL-f contains some unique analytic tools as well. These include the ability to calculate explicitly the probability of any event in the tree and to perform fault tree-specific types of sensitivity analysis. DPL-f provides an interface for incorporating time series into a model. This allows the modeler to account for devaluation, capital

Table 1. The Selected Tools' Capabilities Summary

Selected Tool	Functional Capabilities	
ANSSR (Analysis of Networked Systems Security Risks) MITRE Corporation	*Passive data gathering* - Model structure - Survey based data gathering - Network aware	*Risk Type* - Single Occurrence of Loss
RAM (Risk Assessment Model) NSA	*Passive data gathering* - Event tree - Prioritized attack list *Risk Type* - Mathematical model - Multiple risks/services - Event based over time	*Extensible to Risk Type* - Comparison of effectiveness of different designs - Not limited to computers/networks - Optimization of system/cost benefit analysis
ISS Internet Scanner Internet Security Systems (ISS) Corporation	*Active data gathering* - Scans network for hosts, servers, firewalls, and routers - Assesses security and policy compliance of networks, operating systems, and software applications	*Risk Type* - Computer Network Compliance Report (snapshot in time)

growth, or other time-varying quantities without changing the structure of the model. DPL-f provides RAM with additional capabilities for rapid fault tree construction, libraries of embedded fault trees, an expert opinion generation system, enumeration and ordering of cut sets, and a graphical portrayal of risk over time.

II.3 Output Report Correlation and Generation

None of the above tools take an aggregate snapshot approach to the system, with a "drill down" or layered approach to address risk at various layers (network, platform, database, etc.) of the system. Using multiple risk analysis tools would allow various aspects of the system to be analyzed for vulnerabilities without the cost of developing one tool to perform all types of analysis. To provide a more comprehensive vulnerability assessment of a system than any one tool could provide, the outputs of the various tools must be integrated and fused into a single, concise report. This provides greater assistance to system designers analyzing alternatives among security risk, system performance, and mission functionality.

Under the NVT effort, Harris investigated technologies that would support our goal of integrating and fusing the results from multiple vulnerability analysis applications. By examining the variety of current COTS and GOTS products, and the variety of inputs and outputs those products require, it became apparent that fuzzy decision technology offered the most flexible solution to our problem. Our focus on fuzzy decision methodologies as our technological foundation was based on an analysis of a variety of technologies, including Expert Systems, Databases Systems, Neural Networks, Fuzzy Logic, and Fuzzy Expert Systems. Fuzzy Expert Systems are based on the premise that multi-criteria, multi-expert decision making can lead to a best-fit answer. The primary benefit of a fuzzy reasoning system is its ability to use and assimilate knowledge from multiple sources. We believe that Fuzzy Expert System technology is most applicable to the NVT architecture because:

- At least one expert exists for each tool that we wish to include in the system
- The problem itself is fuzzy; it has ambiguities and often partial information
- We can incrementally learn and apply new technologies as the system grows
- We believe we can identify valid membership functions for the mapping of data to concept and concept to knowledge

NVT performs *FuzzyFusion™* to combine the results of multiple vulnerability assessment/risk analysis tools into a unified report. The *FuzzyFusion™* is accomplished through the use of a Fuzzy Expert System, which combines the outputs of the various tools, user concerns about system risks and vulnerabilities, and expert understanding of the results of each tool and how these fit into the larger information system security picture.

Output of the concise assessment can be provided to the NVT user through multiple means and in various degrees of detail, as illustrated in Figure 4. The graphical network map of a system can be color-coded to provide a visual indication of where the greatest risks are located. In Figure 5, the node with the greatest associated risk is colored red. Less severe risks are colored yellow. A pop-up slider window can also be used to indicate the top *N* risks, and their severity. Further details, such as text reports and spreadsheet analyses, can be accessed by drilling down through the layers of information.

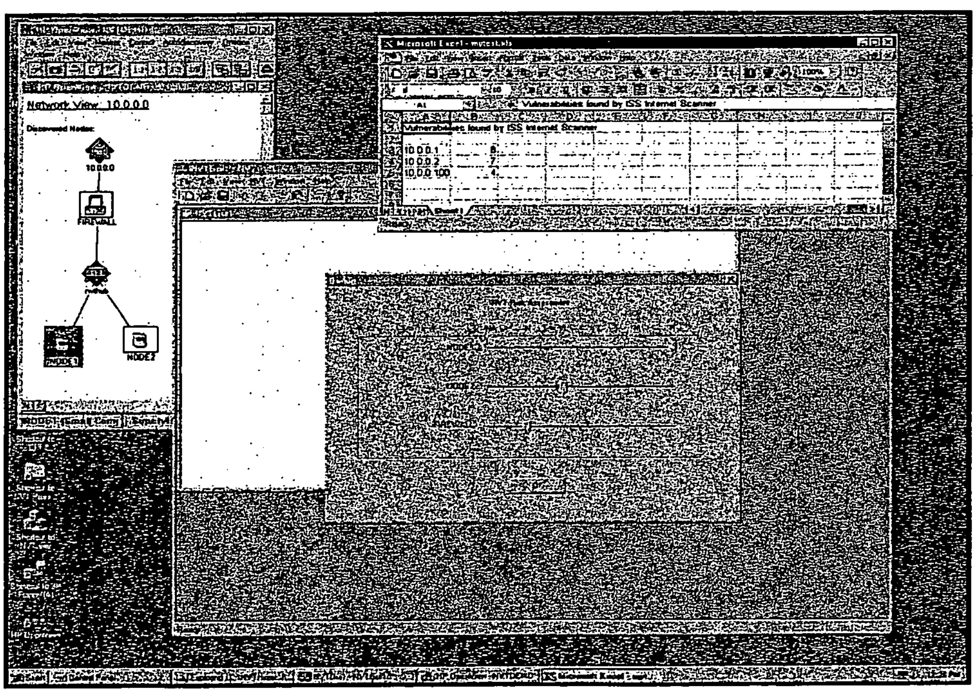


Figure 4. NVT leverages Existing Vulnerability Assessment Tools to present a Single Cohesive Risk Picture

III. FEATURES AND BENEFITS OF NVT

The result of the NVT Program is a prototype demonstrating a comprehensive vulnerability profile based on the user's defined acceptable risk of compromise to a given system. End users have a simple expression of the *vulnerability posture* of a given system or system design, and are capable of performing *"what if"* analysis for functionality, performance, and countermeasure trades.

The primary advantage of the NVT prototype is that it provides a flexible, modular, extensible approach to vulnerability assessment. This innovative design accommodates multiple risk assessment techniques, but only requires single entry of the system description (through auto discovery or manual entry of a model), which is a significant benefit to the System Security Engineer. Figure 5 illustrates the NVT interface to ANSSR. In stand-alone use, ANSSR uses a character based GUI for user data input. As the number of windows and menus suggests, entry of information into the tool is a manually intensive exercise. One of the benefits of NVT is that it automatically provides the required system information to the various vulnerability assessment tools, allowing each tool to use only the input data it requires. NVT eliminates the labor-intensive methods associated with using the legacy assessment tools while preserving the existing user investment in legacy methodologies. NVT also provides a mechanism to correlate information among several tools. Information solicited from the user for any single tool is shared among all tools. Legacy vulnerability assessment tools and databases can be reused, and their results used in conjunction with alternate risk models.

NVT was designed to be an affordable vulnerability assessment environment. Many monolithic risk assessment tools require high performance Unix platforms and cost over $40,000 per copy. The NVT prototype was developed on a Windows NT-based Pentium platform. Our initial tool suite reflects a desire to be economical and pragmatic in tool selection. Three COTS/GOTS vulnerability assessment tools are incorporated into the framework: ANSSR, RAM, and ISS Internet Scanner. Costs for the runtime licenses of COTS products currently employed within the NVT prototype along with a suitable NT workstation are approximately $12,000.

The modular, extensible system design for NVT ensures ease of technology transition and integration as new vulnerability tools and technology vulnerabilities come to market. Our estimate for the incorporation of new tools into the NVT environment is approximately eighty hours of engineering integration. This modularity preserves user legacy models and tool investments, allowing each user to select the tools most appropriate for his environment and needs.

IV. COMPARISON WITH OTHER WORK

To the best of our knowledge, no current risk assessment tool environment is designed as an *integrable architecture*. Most tools on the market today either perform real time, active scanning analysis of a single node within a network, or ask for user input on the network system and its physical environment. Each of these

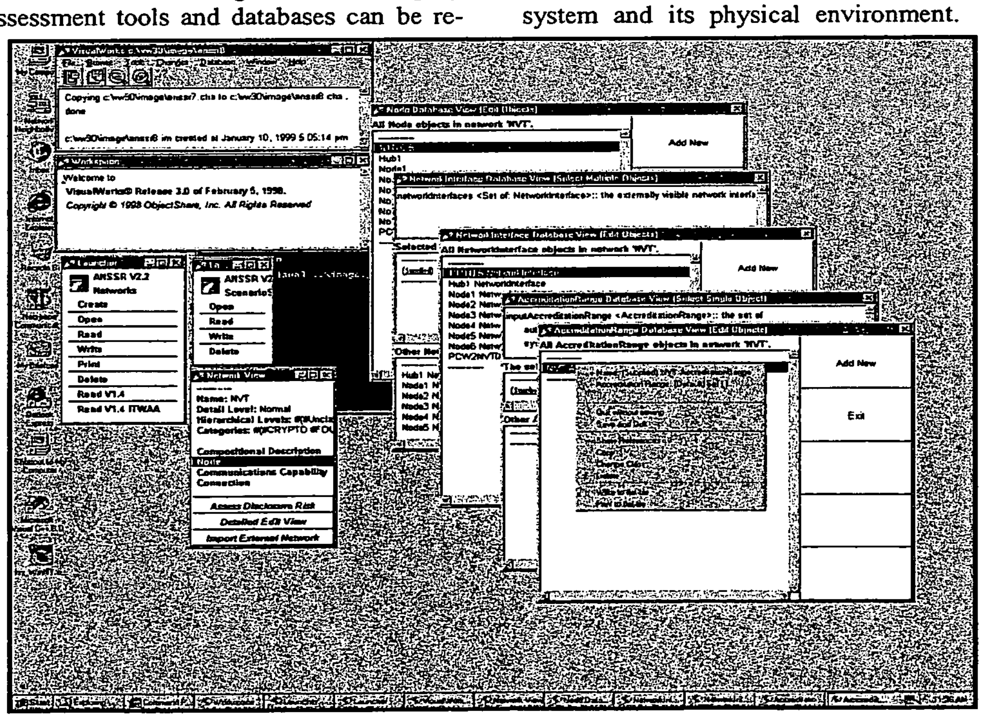


Figure 5. Entering System Information into the Interface for ANSSR is a Manually Intensive Process

techniques is valuable for a particular class of problems. However, the ability to accommodate new protocols, vulnerabilities, and classes of devices within a single risk assessment framework is extremely valuable. NVT also provides a comprehensive graphical output capability that consolidates multiple tool outputs into a cohesive system risk profile. NVT was designed to make risk assessment a feasible, comprehensible activity without requiring the user to develop comprehensive expertise in the interpretation of risk analysis results.

The only tool suite that is as ambitious as NVT is CRAMM, the Central Computer and Telecommunications Agency's (CCTA) Risk Analysis Management Methodology. CRAMM allows security assessments to be conducted in terms of security objectives (policy statements), security functions (countermeasures), or security examples (implementations). CRAMM is designed to be a comprehensive risk assessment system. As such, it is not designed for casual users, but for trained risk analysis experts with a high degree of expertise in the use and interpretation of CRAMM results.

V. FUTURE RESEARCH

The basic foundation of NVT provided valuable experience in risk analysis tool integration and correlation technologies. Future research and development efforts will benefit from the use of the NVT prototype by System Security Engineers. These uses will include applying NVT to:

- Identify vulnerabilities and enforce good security design principles
- "Snapshot" a system and its vulnerabilities, and compare how risk evolves over the system lifecycle
- Correlate information from various risk tools in an understandable graphical vulnerability analysis
- Support hypothetical analysis, facilitating architecture choices among security, functionality, performance, and availability
- Provide rapid specification of the relevant characteristics of a system design

Beyond the efforts conducted under the initial NVT Program, further research is need to improve the ***Fuzzy-Fusion***™ used to combine outputs from various risk analysis tools into a unified report. In addition, we have identified new functionality to incorporate into the results analysis, including:

- **Temporal Based Reasoning**. Accounts for the time required to exploit a known vulnerability as part of the system assessment process. It enables an analyst to perform a vulnerability assessment that accommodates the time required to exercise a given vulnerability. For example, if the time that is required to compromise a given node is greater than the timeline for mission completion, then the threat is minimal.
- **Vulnerability Thresholding**. Minimizes continued computation when an aggregate vulnerability level in a given system or segment exceeds a user defined limit, allowing the user to define his own vulnerability tolerance. It eliminates possibly computationally intensive search trees when a sufficiently lethal vulnerability is located, or when a large number of vulnerabilities are identified. It allows the user to define his vulnerability tolerance level and supports configurable definitions of acceptable levels of vulnerability.
- **Reasoning with uncertainty or incomplete data information**. Provides the user with some answer, usually the best solution that is available with the information available at a given moment in time.
- **Vulnerability trade-off visualization techniques**. Allow the user to easily perform what-if analysis and experimentation among performance, functionality, and countermeasures. It enables the user to readily understand the possible comparisons among desired capabilities.

This functionality will allow NVT to more accurately reflect the human decision making process. Further, it will support a more robust, systems orientation towards vulnerability analysis, accommodating consideration of application and platform vulnerabilities as well as conventional network vulnerabilities.

VI. REFERENCES

- "Comparison of COTS Network Management Tools For Knowledge Solicitation". Network Visualization Tool Program – Task 1 Report. Harris Corporation. Melbourne, Florida. September 1997
- "Comparison of COTS Vulnerability Assessment/Reasoning Engines for Automated Reasoning". Network Visualization Tool – Task 3 Report. Harris Corporation. Melbourne, Florida. October 1998.
- "A Practitioner's View of CRAMM". Norman Truman. Gamma Secure Systems Limited. http://www.gammassl.co.uk/topics/hot5.html. September 1997.
- "Sniffing Out Network Holes". Leslie O'Neil and Joe Scambray. *INFOWORLD*. February 8, 1999. Pp. 74-82.
- "L-3 Network Security Expert 3.0". Product review, *SC Magazine* (Information Security News). http://www.infosecnews.com/13/13.html.
- *Analysis of Networked Systems Security Risks (ANSSR) Assessment Tool, Version 2.2, User's Manual.* D. J. Bodeau and F. N. Chase. The MITRE Corporation. Bedford, MA.
- "ANSSR: A Tool for Risk Analysis of Networked Systems". D. J. Bodeau, F. N. Chase, and S. G. Kass. *Proceedings of the 13th National Computer Security Conference*. October 1990.
- *DPLf User Manual.* Applied Decision Analysis LLC. 1999.
- *ISS Internet Scanner User Guide for Windows NT.* Internet Security Systems (ISS). Atlanta, GA. 1997.

- *HP OpenView for Windows: Workgroup Node Manager User's Guide*. Hewlett Packard. Cupertino, CA. 1998.
- *HP OpenView: Professional Suite Getting Started Guide*. Hewlett Packard. Cupertino, CA. 1998.